Democracy Suite 5.5A

The Dominion Voting Systems Democracy Suite 5.5A election system was examined in Austin on January 16-17, 2019. It is a mainly a paper-based optical scan voting system with an optional DRE with VVPAT precinct voting device. The 5.5A release was certified by the U.S. Elections Assistance Commission in September 2018.

Table 1 - Major Proprietary/COTS Hardware Components

Name	Version/Firmware #	Type
ImageCast Precinct (ICP)	PCOS-320C	Precinct Scanner
ImageCast Precinct (ICP)	PCOS-320A	Precinct Scanner
ICP Ballot Box	BOX-330A	Ballot Box
ICP Ballot Box	BOX-340C	Ballot Box
ICP Ballot Box	BOX-341C	Ballot Box
ICX Tablet (Classic) - aValue 15" COTS Tablet	(SID-15V)	Ballot Marking Device
ICX Tablet (Classic) - aValue 21" COTS Tablet	(SID-21V)	Ballot Marking Device
ICX Tablet (Classic) - aValue 21" COTS Tablet	(HID-21V)	Ballot Marking Device or DRE
Thermal Printer	SII RP-D10	Used with Ballot Marking Device
Thermal Printer	KFI VRP3	Used for VVPAT with DRE
Dell Server	PowerEdge R630	EMS server used for Standard (client server) configuration
Dell Server	PowerEdge R640	EMS server used for Standard (client server) configuration
Dell Server	Precision T3420	EMS server used for Express configuration
ICC Scanner	Canon imageFormula DR-G1130	Central count scanner
ICC Scanner	Canon imageFormula DR-M160II	Central count scanner

Table 2 - Major Proprietary/COTS Software Components

Name	Version/Firmware #	Component of
Election Event Designer (EED)	5.5.12.1	EMS
Results Tally and Reporting (RTR)	5.5.12.1	EMS
EMS Application Server	5.5.12.1	EMS
File System Service (FSS)	5.5.12.1	EMS
Audio Studio (AS)	5.5.12.1	EMS
Data Center Manager (DCM)	5.5.12.1	EMS
Election Data Translator (EDT)	5.5.12.1	EMS
ImageCast Voter Activation (ICVA)	5.5.12.1	EMS
Smart Card Helper Service (SCHS)	5.5.12.1	EMS
Adjudication Services	5.5.8.1	EMS
Election Firmware	5.5.3-0002	ICP
Microsoft SQL Server Database Engine	2016 SP1	EMS
SQLite Database Engine	1.0.103.0	EMS
Microsoft Windows Server OS	2012 R2	EMS
Microsoft Windows OS	10 Professional	EMS and ICC
OpenSSL FIPS Object Module	2.0.14 (Cert 1747)	EMS
Kernel (uClinux) (modified COTS OS)	5.5.3-0002	ICP
ICX Application	5.5.10.25	ICX
Android OS	5.1.1	ICX Classic
Android OS	4.4.4	ICX Prime
Machine Configuration File (MCF)	5.5.10.20_20180806	ICX configuration
ImageCast Central Application	5.5.3.0002	ICC
Device Configuration File (DCF)	5.4.01_20170521	ICP and ICC configuration
OpenSSL FIPS Object Module	2.0.10 (Cert 1747)	ICP and ICC

For a complete detailed listing of the hardware components and software used in the 5.5 system please refer to the EAC certification Scope of Certification here.

Findings

- The Technical Data Package (TDP) documentation provided appears to be accurate and complete.

- The system software was successfully built and the release numbers on the devices and the EMS were verified to match the releases that were used for the EAC testing. There are methods that a jurisdiction can use to verify that the executable programs are unmodified via hash codes. The methods are described in the document *SystemIDGuide-5.5.pdf* for each device, and the EMS. The methods are fairly simple except for the ICX Classic voting machine which requires disassembling the tablet. I do not believe the ICX Classic validation will be performed due to the difficulty and risk of breaking the device.

- The pre-marked and the manually voted test ballots were recorded and tallied correctly.

- The EMS server utilizes a raid 10 self-encrypting disk array. The server is also hardened, including preventing networking, except for a LAN. The EMS database is Microsoft's SQL server. MS-Access ODBC is used for the client-server connectivity.

- Neither by the ballot definition, or a setting on the precinct devices can prevent voting outside of the permitted time frame. Therefore, it is critical that a poll-worker verifies that the date and time are accurate on each device so that the log timestamps are correct.

- Voter activation cards can be program manually for each voter, or automatically by an epollbook. An epollbook laptop should not be connected to a LAN or WAN. Voter activation cards can only be used for a single voting session. The cards must be reprogrammed to be used for another voting session. This prevents a voter from voting more than 1 ballot.

- Adjudication can be done per race, per ballot in the EMS. Images from the voting devices can be viewed on screen. During the examination, the adjudication program had to be restarted because the wrong NAS (network storage) folder path was entered on the ICC system. An error message stating that ballot image cannot be read kept occurring because of the invalid path. This occurred 3 times, requiring a restart each time, until the correct path was entered. (see adjudication error photos at then end of the report) A better design would be to include important paths in the election definition to eliminate human error.

  Overall, the EMS is not as intuitive as it should be. The Dominion reps had trouble using it at times. More training may be needed to use it effectively.

- Ballot images that were scanned on the ICPs were hard to read during adjudication in the EMS. The examiners could not read the write-in names. Pre-printed text was also difficult to read. The low resolution images produced by the ICPs are not suitable for adjudication in the EMS. The ICC ballot images were easy to read during adjudication.

- A poll worker can turn on or off the manual vote session activation on an ICX when the poll is opened. But once the device is opened for voting, the mode of operation cannot be changed without closing and re-opening the poll.

- The voting devices and EMS logs contain the necessary information to aid in auditing the election activity.

  Database and the log files are encrypted which helps to prevent unauthorized, unlogged editing. An attempt to access a log from a file explorer and text editor was unsuccessful.

- The central count LAN utilizes non-routable IP addresses. Regardless, the central-count LAN should not be connected to the internet.

- The ICP precinct scanner can utilize either a collapsible or rolling plastic ballot box. They have 3 bins: regular, write-in, and emergency. Both ballot box styles use security seals.

  The collapsible ballot box emergency slot is a punch-out. If it used because the ICP has an unrecoverable failure, a new ballot box is needed for the next election because the punch-out can not be reattached securely (see photo below).

- The ICP is slow when reading regular ballots (full ballot with marks). Reading and tabulating a ballot took about 8-9 seconds. The CVR/QR coded ballots were read in about 3-4 seconds.

  An ICP can run 2 hours on its internal battery. The ICPs have the required locations for security seals.

  The zero report is printed automatically when a poll worker boots the machine on election day.

- Multiple paper jams occurred on the ICP during the examination. The ICP display indicated that the results were saved, but reported a paper jam. The ballot did not drop into the ballot box. The ICP had to be pulled away from ballot box to get to the ballot. It was then dropped into the box. This would allow poll worker to see the voter's selections.

  This happened 2 times with only 60 ballots processed. Unjamming requires the seal to be broken. Using the protective counter and total paper jams values as seen on the test ICP display (see photo below) the machine has had a paper jam more than 1% of the ballots cast. In a real election, when typically more than a 100 ballots are cast, the jamming could become a problem regarding ballot secrecy and seal management.

- The ICC scanner can read both summary CVR/QR ballots and regular pre-printed voted ballots.

  In the standard configuration, the EMS server provides LAN connectivity using the OS's DHCP protocol. An express server configuration has the EMS and database running on a single workstation. For this setup, a managed hardware switch is used to provide DHCP connectivity for the ICC.

  Canon drivers for the ICC had to be loaded from Canon site. They were not from the certified trusted-build.

- The ICXs are configured as either a BMD or DRE in the EMS during the election setup/definition. An ICX cannot be both on election day and cannot be changed at polling location.

  The ICX BMD requires a UPS power brick to sustain its laser printer for 2 hours. The ICX DRE (which includes the VVPAT printer) does not require it. Power is provided from the tablet to the printer.

  When using an ICX for early-voting, the ICX is put in a suspended mode each night. A poll worker should record the public and protected counters.

  The ICXs are built with a COTS tablet and printer. The Android OS versions used on the tablets are several years old, therefore they do not have the latest security feature as later Android releases. The Dominion representative said the Android versions are provided by the tablet manufacturer, therefore Dominion has no other option.

- The BMD ICX printer can print on both sides of the 14" paper. This should be enough for all of a voters selections. In any case, it is the CVR's QR code that is read by an ICP or ICC scanner to process the ballot.

  The ICX BMD does not have the functionality to print serial numbers on the ballot stock or ballot images. Pre-printed serial numbers on blank ballot stock is the recommended solution. This could be expensive and difficult to manage.

  An ICX DRE can support 200-300 ballots cast on a single VVPAT paper roll. The exact number of ballots depends on the number of races/propositions voted. This should be adequate. If necessary another ICX/DRE can be deployed, or the VVPAT tape can be replaced.

  A spare VVPAT printer can be used instead of replacing a tape roll. There is a "pigtail" connection that allows the VVPAT printer to be replaced without having to break a security seal. Unfortunately, this also allows a voter (or their child) to disconnect the printer since the pigtail is not secured. During testing the VVPAT printer was disconnected at the pigtail in the middle of a voting session. Rebooting the ICX did not restore functionality. It could not be used again until the battery was pulled out of the machine (requires breaking seal). The examiners verified that no votes were lost once functionality was restored.

- If straight-party is selected on an ICX BMD, a voter cannot no-vote any partisan race. If a voter deselects an auto-selected partisan candidate, a vote will still be counted for that candidate (see photo below). Voters may not realize this.

  If a voter selects a candidate that is not in the party of the straight-party selection, all the other auto-selected partisan choices are deselected.
- The ICX/DRE CVRs are transferred to the EMS via a thumb drive. The CVR's QR codes are scanned to tally.

- The ICP and ICC machines required the I-button dongle and the correct passcodes to access the poll worker and administration functions. The ICX DRE and BMD machines require smart cards and passcodes.

- The accessibility testing was done by the SOS staff. The problems reported were:

  Non-audio voting (i.e. sip and puff and paddles) lacked good written instructions on the screen.

  The ICX/BMD the test voter got to the end of the ballot and was not able to cast the ballot because the paper tray for the laser printer was ajar. All selections were lost. If this occurred during an election, the voter would have to get a poll worker to fix the printer and then restart the voting session. This is likely to be an issue for non-accessibility voting sessions too.

Conclusion

There are several critical issues with the Democracy Suite 5.5A release. The major issues are (Form 101 requirements are in bold) :

- The inability to check a straight-party and then no-vote a race and retain the straight-party selections. ***(10) Is capable of permitting straight-party voting.***

- The vulnerability of the ICX/DRE machine because of the pigtail connection to the VVPAT printer. ***(2) Is suitable for the purpose for which it is intended.***

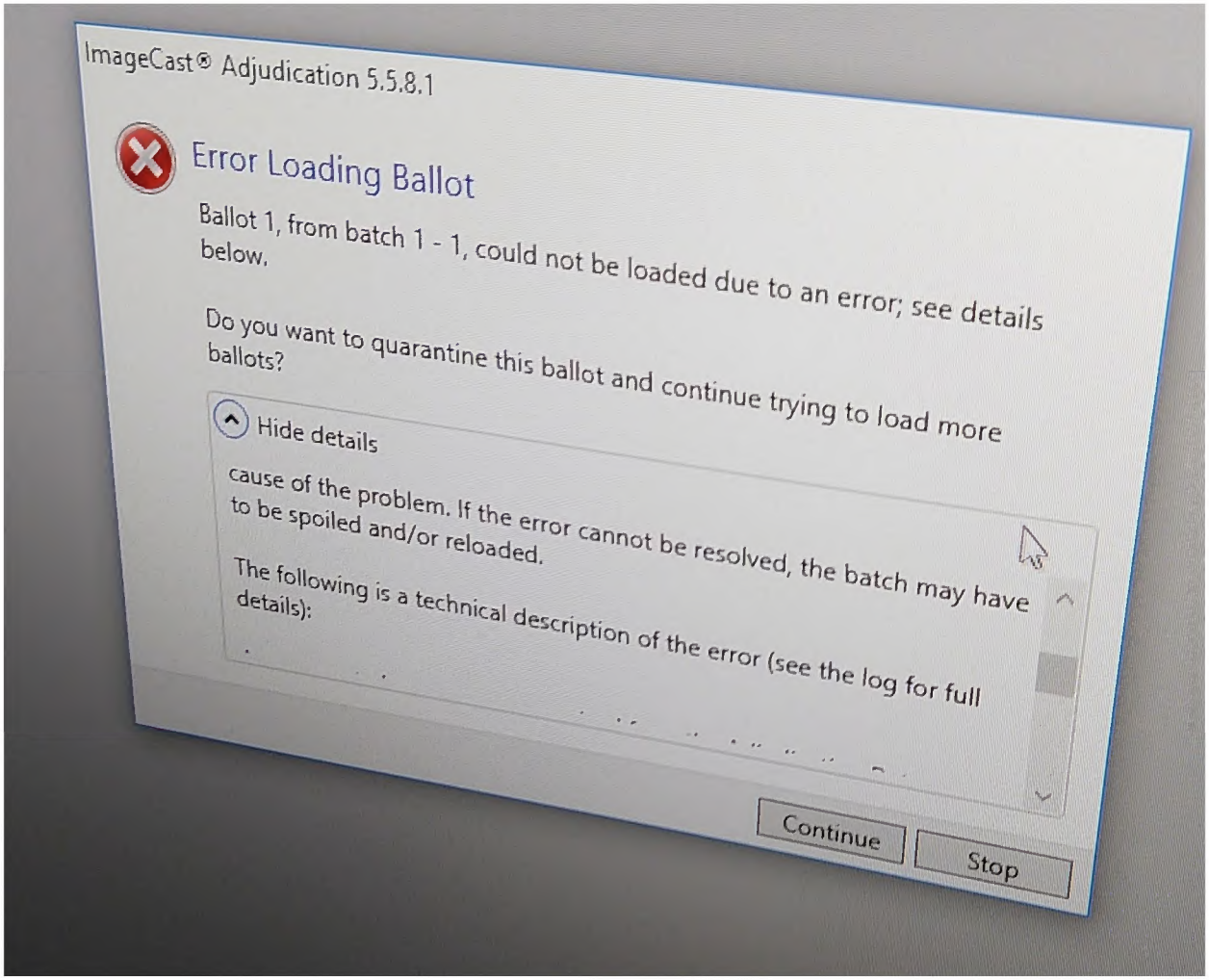
- The error-prone use of the EMS by Dominion reps indicates that it is non-intuitive and could be difficult for a jurisdiction to master. The wrong folder path error (see bullet above) encountered during adjudication is one example. ***(2) Is suitable for the purpose for which it is intended.***

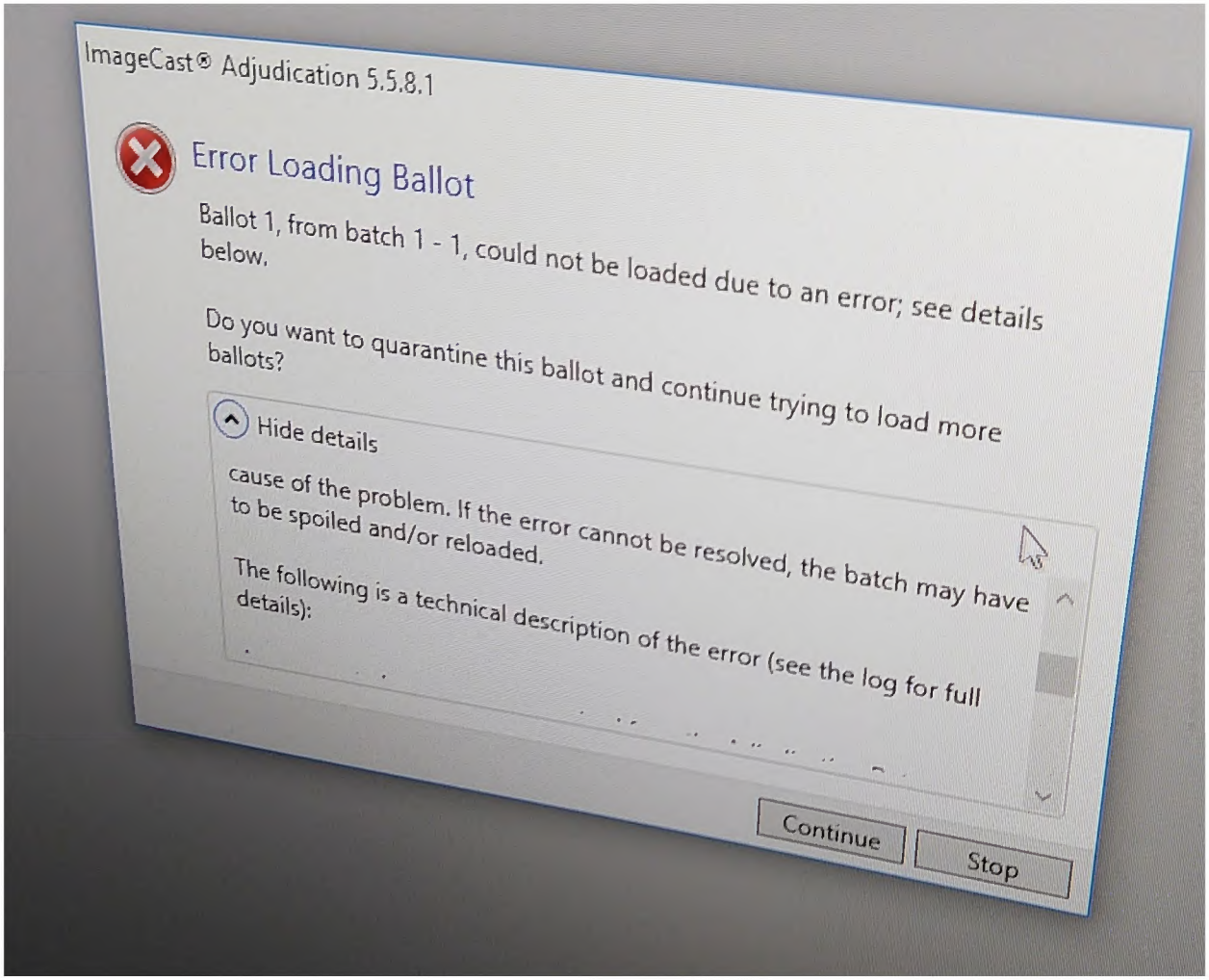
- The poor resolution of the ICP images for use in adjudicating ballots in the EMS, and the poor throughput when reading the regular ballots. ***(2) Is suitable for the purpose for which it is intended.***

- The ICP paper jams (requiring a seal to be broken to unjam it) allowing a poll worker to see a voter's selections. ***(1) Preserves the secrecy of the ballot.***

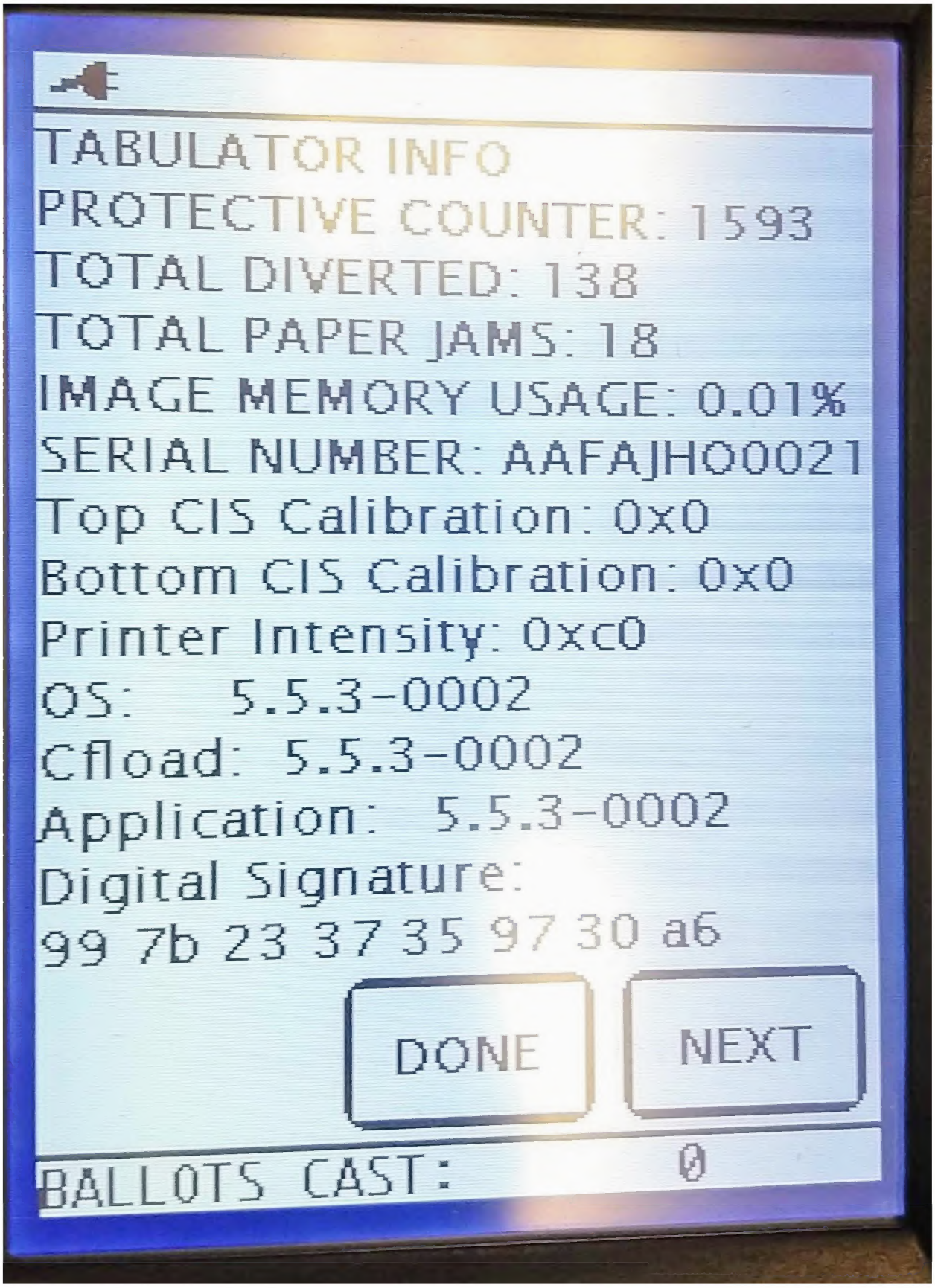
The issues can be fixed, but I believe the system as presented, does not meet the standards required by the Texas Election Code. I **do not** recommend that the Dominion Democracy Suite 5.5A be certified.

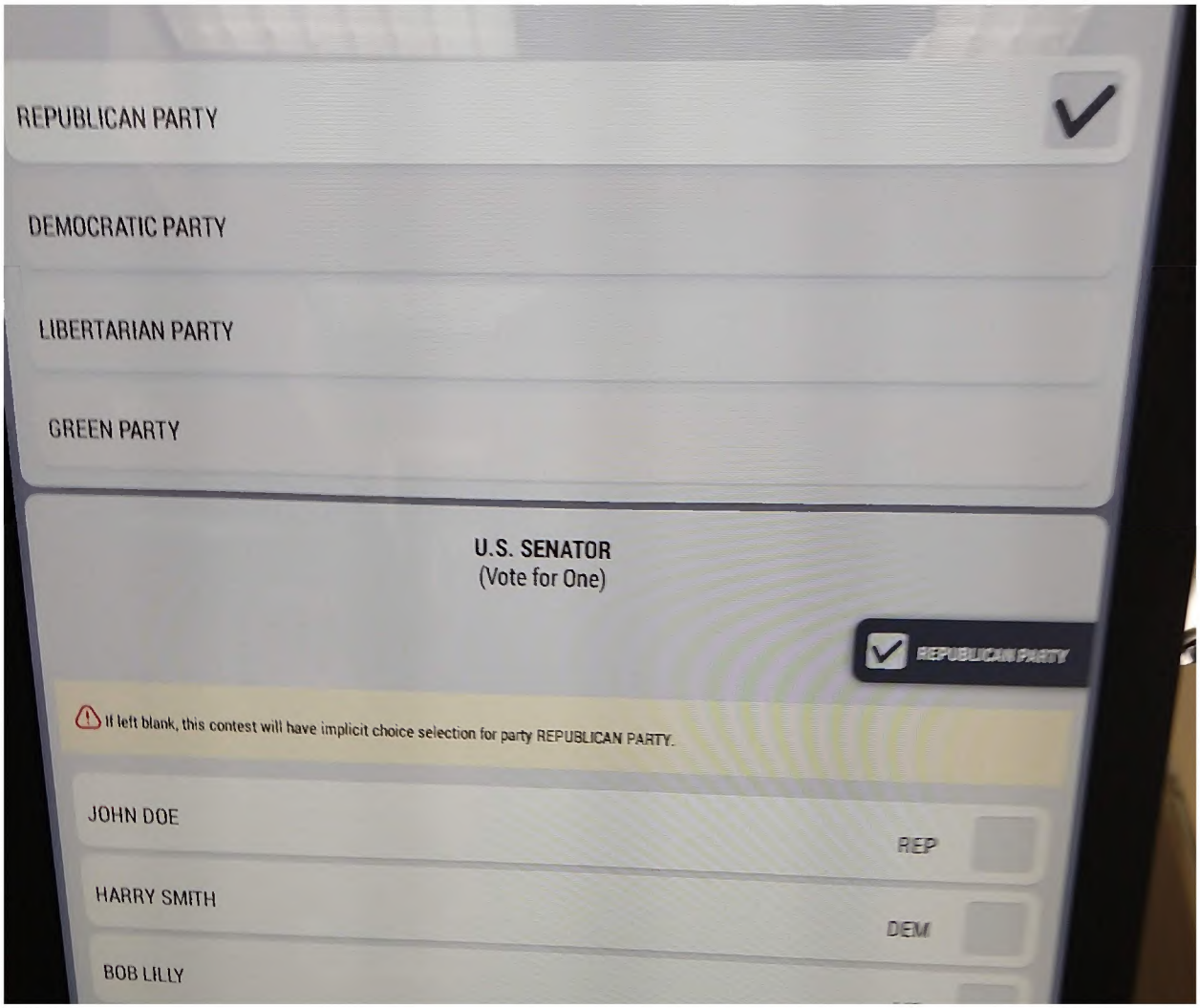
Tom Watson
SOS Examiner


ImageCast® Adjudication 5.5.8.1
Error Loading Ballot
Ballot 1, from batch 1 - 1, could not be loaded due to an error; see details below.
Do you want to quarantine this ballot and continue trying to load more ballots?
Hide details
cause of the problem. If the error cannot be resolved, the batch may have to be spoiled and/or reloaded.
The following is a technical description of the error (see the log for full details):
Continue
Stop


ImageCast® Adjudication 5.5.8.1
Error Loading Ballot
Ballot 1, from batch 1 - 1, could not be loaded due to an error; see details below.
Do you want to quarantine this ballot and continue trying to load more ballots?
Hide details
cause of the problem. If the error cannot be resolved, the batch may have to be spoiled and/or reloaded.
The following is a technical description of the error (see the log for full details):
Continue
Stop


CONSOLE
CF
CF
IN CASE OF POWER FAILUR
PLACE VOTED BALLOTS HE


TABULATOR INFO
PROTECTIVE COUNTER: 1593
TOTAL DIVERTED: 138
TOTAL PAPER JAMS: 18
IMAGE MEMORY USAGE: 0.01%
SERIAL NUMBER: AAFAJH00021
Top CIS Calibration: 0x0
Bottom CIS Calibration: 0x0
Printer Intensity: 0xc0
OS: 5.5.3-0002
Cfload: 5.5.3-0002
Application: 5.5.3-0002
Digital Signature:
99 7b 23 37 35 97 30 a6
DONE
NEXT
BALLOTS CAST: 0


REPUBLICAN PARTY
DEMOCRATIC PARTY
LIBERTARIAN PARTY
GREEN PARTY
U.S. SENATOR
(Vote for One)
REPUBLICAN PARTY
If left blank, this contest will have implicit choice selection for party REPUBLICAN PARTY.
JOHN DOE
REP
HARRY SMITH
DEM
BOB LILLY